What is claimed is:
[1. A copy prevention method of a digital magnetic
recording/reproducing system comprising:
an audio and video signal transmitting process of encrypt-
ing a marker formed by a control word for scrambling
audio and video bit strips and copy prevention infor-
mation for preventing an illegal copy by means of an
encoding key, and multiplexing said marker with said
audio and video bit strips scrambled by said control
word, and
an audio and video signal receiving/recording process of
detecting said marker from said transmitted bit strips,
decrypting and analyzing the detected marker by means
of an encoded key to determine whether copy is per-
mitted or not, updating said detected marker to be
recorded on a video tape, and generating said control
word from said marker to perform a descrambling and
supply the audio and video signals to be displayed on
a monitor.]
[2. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 1.
wherein said marker is placed on a transport-private-data
field within said bit strips.]
[3. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 2.
wherein said marker is comprised of a copy prevention
information area recorded with said copy prevention infor-
mation for preventing said illegal copy, and a control word
area recorded with said control word for descrambling.]
[4. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 3.
wherein said marker is formed of 8 bytes.]
[5. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 4,
wherein said copy prevention area is formed of one byte.]
[6. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 4,
wherein said control word area is formed of four bytes.]
[7. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 3.
wherein said copy prevention information is formatted by
including a generational copy control field for restricting the
number of permitting said copy of a program.]
[8. A copy prevention method of a digital magnetic
recording/reproducing system as claimed in claim 7.
wherein said generational copy control field comprises:
an allowable generational field for restricting the copy
number of said program; and
a current generational field representing a current genera-
tion of a duplicated program.]
[9. A copy prevention-method of a digital magnetic
recording/reproducing system as claimed in claim 1.
wherein said audio and video transmitting process com-
prises:

an audio and video bit-strip encoding step of encoding said audio and video bit strips;

a control word generating step of generating said control word for scrambling;

a scrambling step for scrambling said encoded audio and video bit strips by means of said generated control word;

a copy prevention information generating step of generating said copy prevention information for preventing said illegal copy;

a marker generating and encrypting step of generating said marker by means of said generated control word and copy prevention information and encrypting said marker by means of said encoded key; and

a multiplexing and transmitting step of multiplexing to transmit said scrambled audio and video bit strips and encrypted marker.]

[10. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 1, wherein said audio and video signal receiving/recording process comprises:

a marker detecting step of demultiplexing said transmitted bit strips to detect said marker, and decrypting said marker by means of said encoded key;

a marker analyzing step of analyzing said detected marker to determine whether said copy is permitted or not, and detecting said control word;

an audio and video decoding step of descrambling and decoding said transmitted audio and video bit strips by means of said detected control word, and outputting said audio and video signals; and

a marker inserting step of updating said detected marker and encrypting said updated marker by means of said encoded key to insert the result when it is determined that said copy is permitted after analyzing said marker.]

[11. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 10, wherein said marker analyzing step comprises:

a copy prevention information detecting step of detecting said copy prevention information for preventing said illegal copy from said detected marker;

a copy number restricting step of comparing an allowable generation of said allowable generational field and a current generation of said current generational field representing said current generation for restricting the number of permitting said copy of said program within said detected copy prevention information and determining whether said copy is permitted or not-to process the result; and

a control word detecting step of detecting said control word for descrambling from said detected marker.]

[12. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 11, wherein said copy number restricting step comprises:

comparing said allowable generation of said allowable generational field with said current generation of said current generational field to determine whether said allowable generation is below said current generation;

inhibiting said copy when it is determined that said allowable generation is below said current generation; and

permitting said copy when it is determined that said allowable generation is-not below said current generation, and proceeding to said marker inserting step.]

[13. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 12, wherein said step of inhibiting said copy is performed by destructing said control word or impeding an output of said control word to block a reproduction after recording.]

[14. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 10, wherein said control word is periodically changed.]

[15. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 14, wherein said control word is changed in the interval of 0.6 second.]

[16. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 14, wherein said marker is placed on said transport-private-data field within said bit strips whenever said control word is changed.]

[17. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 16, wherein said marker inserting step comprises the steps of:

updating said marker when the analysis of said marker determines to permit said copy;

encrypting said updated marker by means of said encoded key; and

replaceably inserting said encrypted marker with a succeeding marker.]

[18. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 1, wherein said encoded key is transported via a separate transmission line to be stored.]

[19. A copy prevention method of a digital magnetic recording/reproducing system as claimed in claim 18, wherein said encoded key is transported via said separate transmission line for a prescribed time interval.]

[20. A copy prevention apparatus of a digital magnetic recording/reproducing system comprising:

an encrypted marker detecting and inserting part for detecting a marker from input bit strips, and inserting an updated marker to said bit strips to output the result;

a marker analyzing and processing part for decrypting and analyzing the encrypted marker from said marker detecting and inserting part by means of an encoded key, outputting a control word for descrambling said bit strips, and updating and encrypting the decrypted marker by means of said encoded key to output the result;

a buffer part for buffering said control word and updated and encrypted marker from said marker analyzing and processing part, and inserting said updated and encrypted marker in said marker detecting and inserting part; and

a descrambler for descrambling said bit strips provided via said marker detecting and inserting part by means of said control word from said buffer part.]

[21. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said encoded key is transported via a separate transmission line to be stored.]

[22. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 21, wherein said encoded key is transported via said separate transmission line for a prescribed time interval.]

[23. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said marker is placed on a transport-private-data field within said bit strips whenever said control word is changed.]

[24. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 23. wherein said marker is comprised of a copy prevention information area recorded with said copy prevention information for preventing said illegal copy. and a control word area recorded with said control word for descrambling.]

[25. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24. wherein said marker is formed of 8 bytes.]

[26. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 25. wherein said copy prevention area is formed of one byte.]

[27. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 25. wherein said control word area is formed of four bytes.].

[28. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24. wherein said copy prevention information is formatted by including a generational copy control field for restricting the copy number of a program.]

[29. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 28. wherein said generational copy control field comprises:

an allowable generational field for restricting the number of permitting the copy of a program; and

a current generational field representing a current generation of a duplicated program.]

[30. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20. wherein said control word is periodically changed.]

[31. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 30. wherein said control word is changed in the interval of 0.6 second.]

[32. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 30. wherein said marker is placed on a transport-private-data field within said bit strips whenever said control word is changed.]

[33. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 30. wherein said marker detecting and inserting part replaceably inserts said updated marker with a succeeding marker.]

[34. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24. wherein said marker detecting and inserting part comprises:

a marker detecting section for detecting to output said encrypted marker from said input bit strips to said marker analyzing and processing part, outputting a marker detection flag signal for informing of the position of said encrypted marker within said bit strips to said descrambler to be used as a reference signal of initializing said descrambler, and outputting said bit strips; and

a marker inserting section for inserting said updated and encrypted marker from said buffer part to said bit strips from said marker detecting section in accordance with said marker detection flag signal from said marker detecting section to output the result to said descrambler.]

[35. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 24, wherein said marker analyzing and processing part comprises:

a marker decoding section for decrypting said encrypted marker from said marker detecting and inserting part by means of said encoded key;

- a marker analyzing section for analyzing said copy prevention information within said marker from said marker decoding section, and outputting said control word to said buffer part and a control signal for updating said marker when said copy is permitted; and
- a marker updating and encoding section for updating said marker from said marker decoding section in accordance with said control signal from said marker analyzing section, and encrypting said updated marker by means of said encoded key to output the result to said buffer part.]

[36. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 35, wherein said marker analyzing and processing part further comprises an encoded key storage section for storing said encoded key to output it to said marker analyzing section and marker updating and encoding section.]

[37. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 35, wherein said marker analyzing section compares an allowable generation of an allowable generational field with a current generation of a current generational field representing a current generation of a duplicated program to determine whether said copy is permitted or not.]

[38. A copy prevention apparatus of a digital magnetic recording/reproducing system as claimed in claim 20, wherein said buffer part comprises:

a marker buffer for temporally storing said updated and encrypted marker from said marker analyzing and processing part and outputting the result to said marker detecting and inserting part; and

a control word buffer for temporally storing said control word from said marker analyzing and processing part and outputting the result to said descrambler.]

Sub A1

39. A method for transmitting digital data, comprising:

scrambling digital data; and

transmitting the scrambled digital data, identification information, and copy prevention information as part of a data group, the data group including a header and the header including the identification information, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

40. The method of claim 39, wherein the scrambling step scrambles the digital data based on control data such that the control data controls a parameter of the scrambling operation.

Sub A2

41. The method of claim 40, wherein the transmitting step transmits the control data as part of the data group.

42. The method of claim 41, further comprising:

encrypting the control data prior to the transmitting step; and wherein

the transmitting step transmits the encrypted control data as part of the data group.

43. The method of claim 42, wherein the encrypting step encrypts the control data based on a key.

44. The method of claim 39, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

Sub A3

45. A method for transmitting digital data, comprising:

scrambling digital data; and

recording the scrambled digital data, identification information, and copy prevention information as part of a data group, the data group including a header and the header including the identification information, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

46. The method of claim 45, wherein the scrambling step scrambles the digital data based on control data such that the control data controls a parameter of the scrambling operation.

47. The method of claim 46, wherein the transmitting step transmits the control data as part of the data group.

a

48. The method of claim 47, further comprising:

encrypting the control data prior to the transmitting step; and wherein

the transmitting step transmits the encrypted control data as part of the data group.

49. The method of claim 48, wherein the encrypting step encrypts the control data based on a key.

50. The method of claim 45, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital

data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

51. A method of processing protected digital data, comprising:

receiving a data group including identification information, control data and scrambled digital data, the data group also having a header and the header including the identification information, the identification information indicating that at least a portion of the data group has a data structure for copy prevention; and

descrambling the scrambled digital data based on the control data.

52. The method of claim 51, wherein

the receiving step receives copy prevention information as part of the data group, and further including,

performing a copy prevention function based on the copy prevention information.

53. The method of claim 51, wherein

the receiving step receives encrypted control data as part of the data group; and further including,

decrypting the encrypted control data prior to the descrambling step.

54. The method of claim 53, wherein the decrypting step decrypts the control data using a key.

55. The method of claim 51, wherein the copy prevention information includes one of current generation information and allowable generation information, the current

generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

Sub A4

56. A copy protected recording medium having a data structure for controlling a copy prevention operation of a reproducing device, comprising:

a data group area including an identification area, a copy prevention area and a digital data area;

the identification area including identification information indicating that at least a portion of the data group has a data structure for copy prevention;

the copy prevention area including copy prevention information for controlling a copy prevention operation of a reproducing device; and

the digital data area including scrambled digital data.

57. The recording medium of claim 56, wherein the data group area further includes a control data area, the control data area storing control data for descrambling the scrambled digital data.

Sub A5

58. The recording medium of claim 57, wherein the control data area stores encrypted control data.

59. The recording medium of claim 56, wherein the copy prevention information includes one of current generation information and allowable generation information, the current generation information indicating a number of times the digital data has been copied and the allowable generation information indicating a number of permitted copies of the digital data.

60. A method for protecting digital data, comprising:

encrypting control data, the control data having been used to control a parameter of a scrambling operation for scrambling digital data; and

transmitting the scrambled digital data and a marker, the marker including the control data and copy prevention information.

61. The method of claim 60, wherein the transmitting step transmits the scrambled digital data and the marker as a data group.

C1

62. The method of claim 61, wherein the transmitting step transmits identification information as part of the data group, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.

63. The method of claim 60, wherein the copy prevention information indicates a number of permitted copies of the digital data.

64. The method of claim 60, wherein the encrypting step encrypts the control data using a key.

65. A method for protecting digital data, comprising:

encrypting control data, the control data having been used to control a parameter of a scrambling operation for scrambling digital data; and

transmitting the scrambled digital data and the control data as part of a data group, the data group including a header and the header including the control data.

66. The method of claim 65, wherein the transmitting step transmits copy prevention information as part of the data group.

67. The method of claim 66, wherein the copy prevention information indicates a number of permitted copies of the digital data.

C1

68. The method of claim 65, wherein the encrypting step encrypts the control data using a key.

69. The method of claim 65, wherein the transmitting step transmits identification information as part of the data group, the identification information indicating that at least a portion of the data group has a data structure for copy prevention.